Marlon Sousa

4 Followers About

Computação Quântica — Princípios

Marlon Sousa Sep 13, 2020 · 6 min read

$$\left[\frac{-\hbar^2}{2m}\nabla^2+V\right]\Psi=i\hbar\frac{\partial}{\partial t}\Psi$$

Mecânica Quântica

Conceitos básicos de mecânica quântica para entender o processos de computação quântica.

O processo de computação quântica pode ser abstraído por meio dos quatro postulados a seguir.

Postulado 1

O estado de X é denotado por |x>, é um vetor de coluna, por exemplo:

$$\begin{pmatrix} 1/2 \\ i\sqrt{3}/2 \\ 0 \end{pmatrix}$$

$$|\chi\rangle^\dagger = \langle\chi|$$

Transposta conjugada de X

$$(1/2, -i\sqrt{3}/2, 0)$$

Então Obtemos

$$\langle\chi|\chi\rangle = 1$$

e

$$\langle x|y\rangle \leq 1.$$

Postulado 2

A evolução de um sistema quântico fechado é descrito por uma transformação unitária. E se |ψ> é o estado no tempo t, e |ψ'> é o estado no tempo t', então |ψ'> = U|ψ> para um empregador unitário onde U depende apenas de t e t'.

Um operador "Hermitian" é um operador que satisfaz:

$$A^\dagger = A.$$

Operadores comuns usados em qubits são as matrizes de Pauli

$$I, \sigma_x, \sigma_y, \sigma_z$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{Maps: } |0\rangle \to |1\rangle\,;\; |1\rangle \to |0\rangle\,;\; \frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{Maps: } |0\rangle \to i\,|1\rangle\,;\; |1\rangle \to -i\,|0\rangle$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \text{Maps: } |0\rangle \to |0\rangle\,;\; |1\rangle \to -\,|1\rangle$$

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{Maps: } |0\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}};\; |1\rangle \to \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Decorre da equação de Schrödinger para sistemas físicos.

$$i\hbar \frac{d\,|\psi\rangle}{dt} = H\,|\psi\rangle$$

Onde H é um operador Hermitiano fixo conhecido como Hamiltoniano de um sistema fechado.

Postulado 3

As medições quânticas são descritas por uma coleção {Mm} de operações de medição. Esses operadores atuam em um espaço de estado do sistema que está sendo medido. O índice m se refere aos resultados de medição que podem ocorrer no experimento. Se o estado do sistema quântico é |ψ> imediatamente antes da medição, então a probabilidade de que o resultado m ocorra é dada por:

$$p(m) = \langle\psi|\, {M_m}^{\dagger} M_m \,|\psi\rangle$$

E o estado do sistema após a medição é:

$$M_m\,|\psi\rangle$$

Os operadores de medição que satisfazem a equação

$$\sum_m {M_m}^\dagger M_m = I \ .$$

Suponha que

$$|v_1\rangle \, , |v_2\rangle \, , \ldots , |v_d\rangle$$

Então

$$\{M_i \ = \ |v_i\rangle \, \langle v_i|\}$$

Do estado |ψ> nesta medição que iremos obter

$$\frac{|v_i\rangle \, \langle v_i|\psi\rangle}{|\langle v_i|\psi\rangle|}$$

$$|\langle v_i|\psi\rangle|^2 \ .$$

Um projetor é uma matriz Hermitiana com autovalores 0 e 1. O subespaço com valor próprio 1 é o subespaço associado a este operador.

Suponha que:

$$S_1, S_2, \ldots, S_k$$

$$|\psi\rangle = \alpha_1 |\psi_1\rangle + \alpha_2 |\psi_2\rangle + \cdots + \alpha_k |\psi_k\rangle \ ,$$

Postulado 4

O espaço de estado de um sistema quântico composto é o produto tensorial dos espaços de estado dos sistemas físicos componentes. Se tivermos sistemas numerados de 1 a n, e o sistema do número i é preparado no estado |ψi>, então o estado conjunto do sistema total será:

$$|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle .$$

Sejam S1 e S2 espaços de Hilbert com bases |ei>,....,|ek> e |f1>,....|fl> respectivamente. Então o produto do tensor de S1 e S2 denotado como:

$$S_1 \otimes S_2$$

e a um espaço kl-dimensional que consiste em todas as combinações Lineares de todos os pares possíveis de elementos de bases originais, qual de

$$\{|e_i\rangle \otimes |f_j\rangle\}_{i \leq k, j \leq l}$$

$$(|v\rangle \otimes |w\rangle$$

É frequentemente contratado para |v>|w> ou |vw>.

O produto tensorial de dois vetores é o produto de vetores Krnecker.

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \end{pmatrix} \otimes \begin{pmatrix} \frac{3}{5} \\ \end{pmatrix} \quad \begin{pmatrix} \frac{3}{5\sqrt{2}} \\ \frac{4}{5\sqrt{2}} \end{pmatrix}$$

$$\frac{\quad}{5\sqrt{2}}$$

O produto tensorial satisfaz a propriedade de que o produto de dois vetores unitários é um vetor unitário. Tal

$$|v_1\rangle = \sum a_i |e_i\rangle$$

$$|v_2\rangle = \sum b_j |f_j\rangle$$

São 2 vetores unitários

Então:

$$|v_1\rangle \otimes |v_2\rangle = \sum a_i |e_i\rangle \otimes \sum b_j |f_j\rangle = \sum a_i b_j |e_i\rangle |f_j\rangle \ .$$

$$||v_1\rangle \otimes |v_2\rangle|^2 = \sum |a_i b_j|^2 = \sum |a_i|^2 \sum |b_j|^2 = ||v_1\rangle|^2 \, ||v_2\rangle|^2$$

Outra propriedade importante é que o produto tensorial contem vetores que não são produtos tensores próprios. Por exemplo, pode ser facilmente verificado que o vetor.

$$\frac{1}{\sqrt{2}}(|e_1\rangle |f_2\rangle - |e_2\rangle |f_1\rangle)$$

Não é um produto tensorial em si. Esses vetores são chamados de “entangled”.

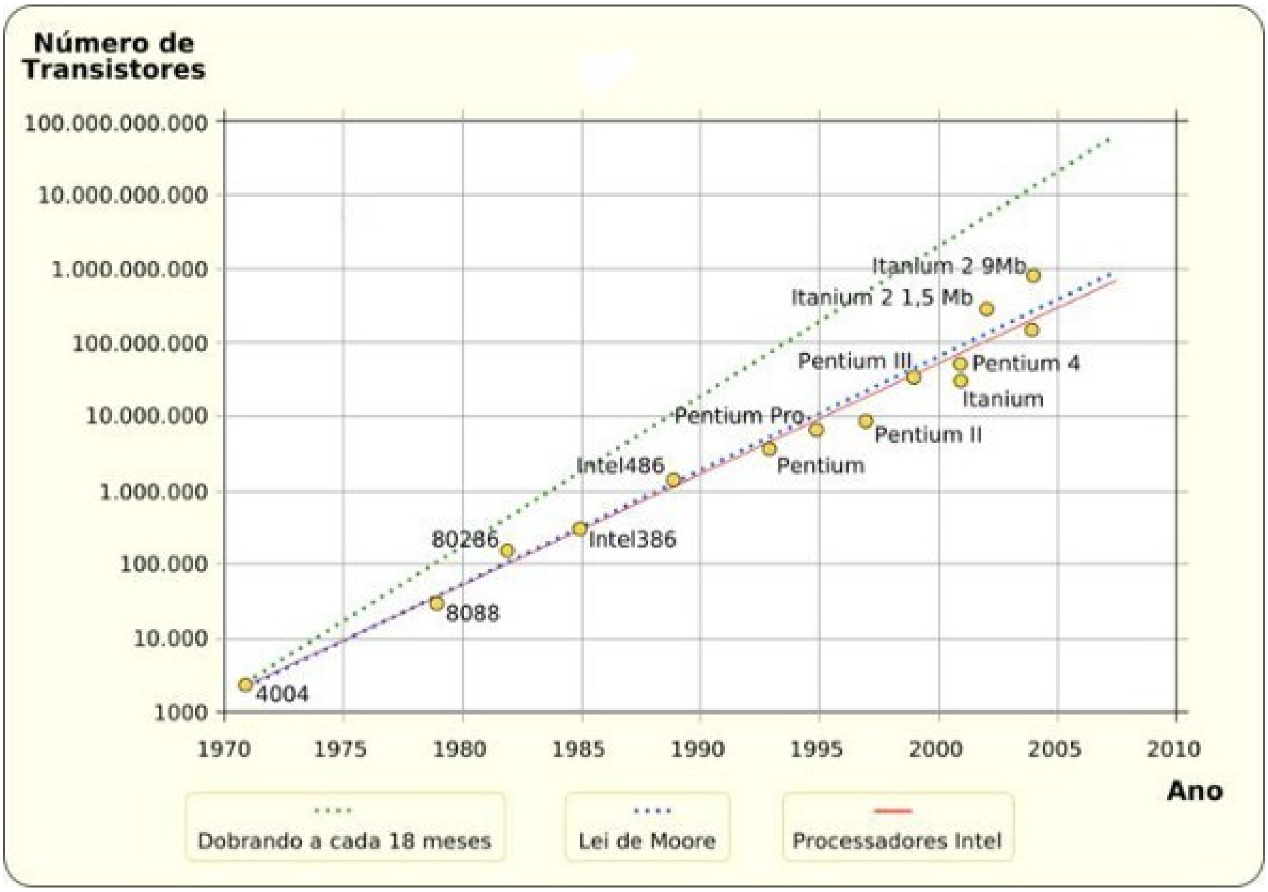
Computação Quântica básica

Um bit pode ter até 2 valores: 0 ou 1, e tudo que vemos em nossa computação cotidiana são apenas 0 e 1.

Nossos computadores atuais funcionam para cálculos em longos, mas nossos processamentos estão cada vez mais lentos para o que precisamos realizar, depende desse algo que pode levar muito tempo. Qubrar um Hash de uma senha é um exemplo de limitação que tempos hoje, no entanto, também estamos quase no limite de transistores possíveis em um processador.

Lei de Moore

A lei de Moore dita que o número de transistores dobra a cada 2 anos, ou seja, o poder computacional dobra a cada 2 anos. Essa dobra não vai continuar para sempre, e esse fim está previsto para 2025.



Processamento Quântico

Os computadores quânticos assim como os computadores clássicos utilizam pequenas peças de informação, mas ao invés de bit, tempos o qubits que foi mencionado na parte matemática. Qubits significa bit quântico.

um eletron ou átomo. Quando falamos de processamento quântico falamos também da super posição. O bit clássico pode ter apenas 2 valores, 0 e 1, enquanto no processamento quântico, nossos qubits podem ser 0, 1 ou 0 e 1 em super posição.

Ao contrário do que muitos pensam os computadores quânticos não podem ser usados para tudo, pois de acordo com a lei quântica da super posição nós não podemos medir acerto em um qubit em super posição.

Algoritmo de Grover

Em um sistema de processamento clássico para testarmos uma comparação de uma palavra com uma lista de outras palavras onde esta lista contém 1.000.000 de palavras, nosso computador precisaria checar palavra por palavra. Em um processamento quântico nosso algoritmo seria capaz de encontrar uma palavra em menos de segundos, no entanto, a probabilidade desta palavra ser a correta e de 1 em 1.000.000. No entanto a probabilidade e de um sistema quântico está diretamente ligada a intensidade da onda que aquele nome transmite, ou seja, aumentando a intensidade onda da palavra podemos aumentar consideravelmente a probabilidade de nosso algoritmo encontrar a palavra, assim baixando a probabilidade para algo em torno de 1 em 5.000.

Computadores quânticos não são essa “magia” que todo mundo fala, pois a maioria das pessoas não sabem o que é computação quântica.

Quantum Computing Quantum Physics Quantum Mechanics Physics Physicians